

Control de Modificaciones

Revisión	Modificación
13	Cambios a la versión 12
14	Cambios a la versión 13



PROGRAMACIÓN DIDÁCTICA

CICLO FORMATIVO DE GRADO MEDIO / SUPERIOR

IFC201 – SISTEMAS MICROINFORMÁTICOS Y REDES

0226 – SEGURIDAD INFORMÁTICA

CURSO 2022-2023

Elaborado: <i>Alberto Rodríguez Giménez</i>	Revisado y Aprobado: <i>Departamento de Informática y Comunicaciones</i> <i>17-10-2022</i>
--	---



ÍNDICE

1.	INTRODUCCIÓN.....	3
2.	COMPETENCIAS PROFESIONALES, PERSONALES Y SOCIALES.....	4
3.	OBJETIVOS	5
4.	CONTENIDOS.....	6
4.1.	Unidades formativas de menor duración.....	6
4.2.	Unidades didácticas	7
4.3.	Distribución temporal de las unidades didácticas.....	7
4.4.	Contenidos de las unidades didácticas	8
4.5.	Contenidos mínimos.....	11
5.	METODOLOGÍA DIDÁCTICA	12
6.	LA EVALUACIÓN	14
6.1.	Base legal.....	14
6.2.	Relación entre los resultados de aprendizaje y criterios de evaluación	15
6.3.	Instrumentos y procedimientos de evaluación	19
6.4.	Criterios de calificación.....	20
6.5.	Recuperación	21
6.6.	Evaluación de alumnos que hayan perdido el derecho a evaluación continua	22
6.7.	Evaluación final y evaluación extraordinaria	22
6.8.	Evaluación de la práctica docente y del proceso de enseñanza.....	23
7.	ACTIVIDADES DE ORIENTACIÓN Y APOYO ENCAMINADAS A LA SUPERACIÓN DE LOS MÓDULOS PROFESIONALES PENDIENTES.....	23
8.	EDUCACIÓN EN VALORES	24
9.	RECURSOS DIDÁCTICOS Y BIBLIOGRAFÍA.....	24
10.	ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES	25
11.	MEDIDAS DE ATENCIÓN A LA DIVERSIDAD.....	26
12.	PLAN DE CONTINGENCIA.....	27
13.	PUBLICIDAD DE LA PROGRAMACIÓN.....	27
14.	MODIFICACIONES DE LA VERSIÓN 12.....	28
	Anexo I: Adecuación de la programación didáctica antes situaciones derivadas por el COVID-19 (<i>secuenciación de contenidos, metodología didáctica, instrumentos de evaluación y criterios de calificación</i>).....	Error! Marcador no definido.



1. INTRODUCCIÓN

Esta programación ha sido realizada tomando como referencia la ORDEN de 29 de mayo de 2008, de la Consejera de Educación, Cultura y Deporte, por la que se establece la *estructura básica de los currículos* de los ciclos formativos de formación profesional y su aplicación en la Comunidad Autónoma de Aragón, la ORDEN de 26 de octubre de 2009, de la Consejera de Educación, Cultura y Deporte, que regula la *matriculación, evaluación y acreditación académica* del alumnado de Formación Profesional en los centros docentes de la Comunidad Autónoma de Aragón y la ORDEN de 26 de julio de 2009, de la Consejera de Educación, Cultura y Deporte, por la que se establece el *currículo del título de Técnico en Sistemas Microinformáticos y Redes* para la Comunidad Autónoma de Aragón.

El módulo Seguridad Informática pertenece al segundo curso del Ciclo Formativo conducente al título “Técnico en Sistemas Microinformáticos y Redes” y consta de 105 horas.

Los alumnos que acceden a este ciclo tienen diferente procedencia, unos proceden de otros ciclos formativos de grado medio, otros de la ESO, donde han podido cursar la optativa de Informática y otros han accedido mediante la prueba de acceso.

Esta programación está elaborada para llevarla a cabo en un instituto ubicado en una localidad de unos 35000 habitantes.

El instituto dispone de los niveles educativos de ESO, Bachillerato y Ciclos Formativos de Grado Medio y Grado Superior. El número de alumnos es de unos 990 y el nivel sociocultural es en su mayoría medio.



2. COMPETENCIAS PROFESIONALES, PERSONALES Y SOCIALES

La formación del módulo contribuye a alcanzar las siguientes competencias profesionales, personales y sociales:

- Determinar la logística asociada a las operaciones de instalación, configuración y mantenimiento de sistemas microinformáticos, interpretando la documentación técnica asociada y organizando los recursos necesarios. a)
- Instalar y configurar software básico y de aplicación, asegurando su funcionamiento en condiciones de calidad y seguridad. c)
- Ejecutar procedimientos establecidos de recuperación de datos y aplicaciones ante fallos y pérdidas de datos en el sistema, para garantizar la integridad y disponibilidad de la información. i)
- Elaborar documentación técnica y administrativa del sistema, cumpliendo las normas y reglamentación del sector, para su mantenimiento y la asistencia al cliente. j)
- Asesorar y asistir al cliente, canalizando a un nivel superior los supuestos que lo requieran, para encontrar soluciones adecuadas a las necesidades de éste. l)
- Mantener un espíritu constante de innovación y actualización en el ámbito del sector informático. n)
- Aplicar los protocolos y normas de seguridad, calidad y respeto al medio ambiente en las intervenciones realizadas. o)
- Cumplir con los objetivos de la producción, colaborando con el equipo de trabajo y actuando conforme a los principios de responsabilidad y tolerancia. p)
- Gestionar su carrera profesional, analizando las oportunidades de empleo, autoempleo y aprendizaje. t)
- *Resolver problemas y tomar decisiones individuales siguiendo las normas y procedimientos establecidos definidos dentro del ámbito de su competencia. r)*
- *Mantener sistemas microinformáticos y redes locales, sustituyendo, actualizando y ajustando sus componentes, para asegurar el rendimiento del sistema en condiciones de calidad y seguridad. n)*



3. OBJETIVOS

La formación del módulo contribuye a alcanzar los siguientes objetivos generales:

- a) Organizar los componentes físicos y lógicos que forman un sistema microinformático, interpretando su documentación técnica, para aplicarlos medios y métodos adecuados a su instalación, montaje y mantenimiento.
- c) Reconocer y ejecutar los procedimientos de instalación de sistemas operativos y programas de aplicación, aplicando protocolos de calidad, para instalar y configurar sistemas microinformáticos.
- d) Representar la posición de los equipos, líneas de transmisión y demás elementos de una red local, analizando la morfología, condiciones y características del despliegue, para replantear el cableado y la electrónica de la red.
- e) Ubicar y fijar equipos, líneas, canalizaciones y demás elementos de una red local cableada, inalámbrica o mixta, aplicando procedimientos de montaje y protocolos de calidad y seguridad, para instalar y configurar redes locales.
- g) Localizar y reparar averías y disfunciones en los componentes físicos y lógicos para mantener sistemas microinformáticos y redes locales.
- k) Reconocer características y posibilidades de los componentes físicos y lógicos, para asesorar y asistir a clientes.
- l) Detectar y analizar cambios tecnológicos para elegir nuevas alternativas y mantenerse actualizado dentro del sector.
- m) *Reconocer y valorar incidencias, determinando sus causas y describiendo las acciones correctoras para resolverlas*
- j) *Valorar el coste de los componentes físicos, lógicos y mano de obra para elaborar presupuestos*



4. CONTENIDOS

4.1. Unidades formativas de menor duración

El módulo “Seguridad Informática” se divide en dos unidades formativas de menor duración:

UF0226_12. Seguridad informática. Conceptos generales y formas pasivas.

Duración: 45 horas

Conceptos: vulnerabilidad, amenaza, riesgo, ataque y daño.

Aplicación de medidas de seguridad pasiva. Buenas prácticas en:

- Ubicación y protección física de los equipos y servidores.
- Sistemas de alimentación ininterrumpida.

Gestión de dispositivos de almacenamiento:

- Almacenamiento de la información: rendimiento, disponibilidad, accesibilidad.
- Almacenamiento redundante y distribuido.
- Almacenamiento remoto y extraíble.
- Cifrado y Criptografía de datos.
- Copias de seguridad e imágenes de respaldo.
- Medios de almacenamiento.
- Implementación de listas de control de acceso. Cumplimiento de la legislación y de las normas sobre seguridad:
- Legislación sobre protección de datos.
- Legislación sobre los servicios de la sociedad de la información y correo electrónico.

UF0226_22. Seguridad informática. Implementación de formas activas.

Duración: 60 horas

Aplicación de mecanismos de seguridad activa:

- Identificación digital. Firma electrónica y certificado digital. Implementación.
- Seguridad en los protocolos para comunicaciones inalámbricas.
- Tunneling seguro. IPSec. VPN's. SSH.
- Implementación y utilización de cortafuegos en un sistema o servidor.
- Política de contraseñas.
- Recuperación de datos desde copias de seguridad.

- Software malicioso. Clasificación. Herramientas de protección y desinfección.

Aseguramiento de la privacidad:

- Métodos para asegurar la privacidad de la información transmitida.
- Fraudes informáticos y robos de información. Estudio de casos
- Control de la monitorización en redes cableadas.
- Seguridad en redes inalámbricas peculiaridades e implementaciones.
- Sistemas de identificación: firma electrónica, certificados digitales y otros.
- Cortafuegos: funcionalidad básica en equipos y servidores dedicados.
- Zonas desmilitarizadas (redes perimetrales)

4.2. Unidades didácticas

El contenido de la programación se ha dividido en 8 unidades didácticas. La relación secuenciada de Unidades Didácticas es la siguiente:

UD1 Conceptos básicos de la seguridad informática

UD2 Criptografía

UD3 Seguridad pasiva: equipos

UD4 Seguridad pasiva: almacenamiento

UD5 Seguridad activa: sistema operativo y aplicaciones

UD6 Seguridad activa: acceso a redes

UD7 Seguridad activa: control de redes

UD8 Ataques y contramedidas

4.3. Distribución temporal de las unidades didácticas

Durante la primera evaluación, que concluye en diciembre (12 semanas):

UD1, UD2, UD3, UD4 – UD8 Impartida con carácter transversal

Durante la segunda evaluación, que termina en marzo (10 semanas):

UD5, UD6, UD7, UD8 - Impartida con carácter transversal

4.4. Contenidos de las unidades didácticas

Unidad Formativa	Unidades	Tiempo estimado
UF0226_12. Seguridad informática. Conceptos generales y formas pasivas.	1. Conceptos básicos de la seguridad informática	12
	2. Criptografía (*)	10
	3. Seguridad pasiva: equipos	10
	4. Seguridad pasiva: almacenamiento	12
UF0226_22. Seguridad informática. Implementación de formas activas.	5. Seguridad activa: sistema operativo y aplicaciones	16
	6. Seguridad activa: acceso a redes	17
	7. Seguridad activa: control de redes	16
	8. Ataques y contramedidas	12

(*) La unidad 2, "Criptografía" incluye contenidos que están incluidos en la UF0226_22

Los contenidos, de acuerdo con el currículo del ciclo, de cada una de las unidades formativas son:

UF0226_12. Seguridad informática. Conceptos generales y formas pasivas.
<p>Conceptos: vulnerabilidad, amenaza, riesgo, ataque y daño.</p> <p>Cumplimiento de la legislación y de las normas sobre seguridad:</p> <ul style="list-style-type: none"> - Legislación sobre protección de datos. - Legislación sobre los servicios de la sociedad de la información y correo electrónico. <p>Aplicación de medidas de seguridad pasiva. Buenas prácticas en:</p> <ul style="list-style-type: none"> - Ubicación y protección física de los equipos y servidores. - Sistemas de alimentación ininterrumpida.



UF0226_12. Seguridad informática. Conceptos generales y formas pasivas.

Gestión de dispositivos de almacenamiento:

- Almacenamiento de la información: rendimiento, disponibilidad, accesibilidad.
- Almacenamiento redundante y distribuido.
- Almacenamiento remoto y extraíble.
- Cifrado y Criptografía de datos.
- Copias de seguridad e imágenes de respaldo.
- Medios de almacenamiento.
- Implementación de listas de control de acceso.

Dichos contenidos se distribuyen principalmente en las siguientes unidades didácticas:

1.- Conceptos sobre seguridad informática

- ¿Por qué proteger?
- ¿Qué proteger?
- Definiciones
- Tipos de ataques
- Buenas prácticas
- Legislación

2.- Criptografía de datos

- ¿Por qué cifrar?
- Criptografía
- Criptografía simétrica y asimétrica
- PKI. DNle

3.- Seguridad pasiva: equipos

- Ubicación del CPD
- Centro de respaldo
- SAI/UPS

4.- Seguridad pasiva: almacenamiento

- Estrategias de almacenamiento
- Backup de datos
- Imagen del sistema



Nota: los contenidos de la unidad 2 incluyen apartados que pertenecen a la UF226_22, pero se agrupan para formar una unidad didáctica coherente.

UF0226_22: Seguridad informática. Implementación de formas activas

Aplicación de mecanismos de seguridad activa:

- Identificación digital. Firma electrónica y certificado digital. Implementación.
- Seguridad en los protocolos para comunicaciones inalámbricas.
- Tunneling seguro. IPSec. VPN's. SSH
- Implementación y utilización de cortafuegos en un sistema o servidor.
- Política de contraseñas.
- Recuperación de datos desde copias de seguridad
- Software malicioso. Clasificación. Herramientas de protección y desinfección.

Aseguramiento de la privacidad

- Métodos para asegurar la privacidad de la información transmitida.
- Fraudes informáticos y robos de información. Estudio de casos.
- Control de la monitorización en redes cableadas.
- Seguridad en redes inalámbricas, peculiaridades e implementaciones.
- Sistemas de identificación: firma electrónica, certificados digitales y otros.
- Cortafuegos: funcionalidad básica en equipos y servidores dedicados.
- Zonas desmilitarizadas (redes perimetrales)

Dichos contenidos se distribuyen principalmente en las siguientes unidades didácticas:

5.- Seguridad activa: sistema operativo y aplicaciones

- Autenticación en el sistema operativo
- Cuotas
- Actualizaciones y parches
- Antivirus
- Monitorización
- Aplicaciones web
- Cloud computing



6.- Seguridad activa: acceso a redes

- Redes cableadas
- Redes inalámbricas
- VPN
- Servicios de red. Nmap y Netstat

7.- Seguridad activa: control de redes

- Control de red
- Firewall
- Proxy
- Spam

8.- Ataques y contramedidas

- Ataques TCP/IP. MITM
- Ataques wifi. Aircrack-ng
- Ataques web. WebGoat
- Ataques proxy. Ultrasurf

4.5. Contenidos mínimos

El alumno debe alcanzar los cinco resultados de aprendizaje establecidos en el currículo ya que contribuyen a la adquisición de las cualificaciones y competencias profesionales establecidas en el Título.

En el apartado **6.2. Relación entre los resultados de aprendizaje y criterios de evaluación** se recogen los resultados de aprendizaje relacionados con los criterios de evaluación y las unidades didácticas. En dicha tabla se seleccionarán aquellos criterios de evaluación que se consideran mínimos para la consecución del resultado de aprendizaje, destacándolos del resto.



5. METODOLOGÍA DIDÁCTICA

A continuación, se exponen los aspectos generales de la metodología didáctica a utilizar.

Las primeras semanas del curso se procederá a realizar una valoración inicial de los alumnos para conocer su nivel de conocimientos previos y la homogeneidad del grupo. Para ello se les preguntará por los estudios realizados y por las optativas cursadas que tengan relación con la informática. Para la obtención de información se podrán utilizar diferentes técnicas e instrumentos como la observación, la realización de ejercicios o prácticas con los ordenadores, la formulación de preguntas directas o la realización de alguna prueba escrita.

Se pretende potenciar en los alumnos un aprendizaje comprensivo y participativo, la capacidad de aprender a aprender y el trabajo en equipo, proporcionando una visión global de los procesos productivos relacionados con los sistemas informáticos y con las redes de comunicaciones. La estrategia metodológica estará orientada a la adquisición y desarrollo de las cualificaciones y competencias profesionales, lo que implica para el alumno que ha adquirido la base teórica, ha desarrollado las habilidades y, lo que es más importante, es capaz de aplicarlo con la calidad exigida en un contexto social y profesional concreto. Por ello muchas de las actividades de enseñanza-aprendizaje simularán situaciones reales del mundo laboral en las que se pueda evaluar el trabajo realizado por el alumno.

El profesor expondrá cada unidad didáctica apoyándose en el libro de texto, cuyos contenidos se modificarán, si procede, para adaptarlos al currículo del módulo y para adaptarlos a las versiones actuales de software. En función de la materia impartida se propondrá la realización de ejercicios, problemas y/o supuestos prácticos para ser resueltos en el cuaderno o con el ordenador, con el fin de facilitar la comprensión y aprendizaje al alumnado.

La exposición de la materia se realizará, en la medida de lo posible, mediante la proyección de diapositivas, visualización de documentos o vídeos. La pizarra será el recurso más utilizado para la resolución de dudas y realización de determinados ejercicios.

Desde el primer día de clase se fomentará la participación activa del alumno en las mismas, haciendo hincapié en que pregunten todo aquello que no entienden. Al principio de cada clase se dedicará un tiempo para que los alumnos planteen sus dudas o realicen preguntas sobre la materia ya impartida. Las dudas se resolverán individual o colectivamente, según proceda. En este proceso es fundamental la participación del alumno.

En el caso de que los alumnos no pregunten, durante un tiempo razonable, el profesor toma la iniciativa preguntando sobre aquellos conceptos que considera más complejos o que pueden entrañar una mayor dificultad en su aprendizaje. En determinados momentos del curso se preguntará y calificarán las respuestas de los alumnos.



Los alumnos deberán tomar apuntes para completar la materia, así como realizar los trabajos de ampliación de conocimientos apoyándose en materiales diferentes al libro de texto. La búsqueda de información en Internet será habitual a lo largo del todo el curso.

La naturaleza de este módulo supone una fuerte relación con el currículo desarrollado en otros módulos del ciclo, tanto de primero como de segundo curso, por ello se mantendrá una coordinación con el resto de profesores a través del Departamento.

En el presente curso los recursos disponibles en el aula nos conducen a la utilización de máquinas virtuales. Cuando el número de alumnos en la clase lo exija se formarán grupos de dos alumnos por ordenador. En estos casos se propondrá un plan de trabajo que permita a ambos alumnos la utilización de los recursos disponibles. Se intentará incorporar el trabajo colaborativo y el aprendizaje basado en problemas, proyectos o retos.

En cuanto al trabajo desarrollado por el alumno será mixto. En ocasiones predominará el trabajo individual para que el alumno se enfrente a los problemas de seguridad informática y adquiriera cierta autonomía en la resolución de problemas y en el manejo de las herramientas; pero también se propondrán problemas, trabajos o proyectos para ser resueltos en grupo, en cuyo caso el número de alumnos dependerá de la actividad a desarrollar y los agrupamientos se realizarán para fomentar el trabajo en equipo. Algunos de dichos trabajos deberán ser expuestos por los alumnos en clase utilizando herramientas TIC, como las presentaciones o la proyección de vídeos.

Para los alumnos que trabajen agrupados, los trabajos individuales en el aula los resolverán en grupo.

En relación con la organización de los espacios y el tiempo:

- Se velará por el cumplimiento de las normas de uso de los ordenadores y demás herramientas en el aula.
- El horario del presente curso nos permite disponer de horas agrupadas que facilitarán la realización de prácticas más complejas y que precisan más tiempo para ejecutarlas.
- Se han previsto desdobles que permitirán trabajar con la mitad de alumnos 2 de las 5 sesiones semanales del módulo. De esta forma se podrá dar una atención más individualizada.

Los alumnos serán informados de las características del módulo Seguridad Informática y de la normativa que establece el currículo en la primera sesión. Con posterioridad, una vez aprobada por el Departamento, se dará publicidad al contenido de esta programación, haciendo hincapié en aquellos aspectos relacionados con la evaluación. Se llevará control de las faltas de asistencia y retrasos de los alumnos, notificándolas al tutor. En los casos en los que se considere necesario, a través del tutor o del equipo directivo, se contactará con la familia o tutor legal del alumno.



6. LA EVALUACIÓN

6.1. Base legal

Para concretar la evaluación, nos hemos basado en:

- *“Orden del 26 de octubre de 2009, de la Consejera de Educación, Cultura y Deporte, que regula la matriculación, evaluación y acreditación académica del alumnado de Formación Profesional en los centros docentes de la Comunidad Autónoma de Aragón”, aplicable desde el curso 2009-2010 a los ciclos formativos de Formación Profesional.”*
- *ORDEN ECD/409/2018, de 1 de marzo, por la que se modifica la Orden de 26 de octubre de 2009, de la Consejera de Educación, Cultura y Deporte, que regula la matriculación, evaluación y acreditación académica del alumnado de Formación Profesional en los centros docentes de la Comunidad Autónoma de Aragón y la Orden de 8 de mayo de 2014, de la Consejera de Educación, Universidad, Cultura y Deporte, por la que se regula las enseñanzas de los ciclos formativos de Formación Profesional y enseñanzas deportivas en la modalidad a distancia en la Comunidad Autónoma de Aragón.*
- *RESOLUCIÓN de 6 de marzo de 2018, del Director General de Planificación y Formación Profesional, por la que se dictan instrucciones para la ejecución y aplicación el desarrollo de la Orden de 26 de octubre de 2009, de la Consejera de Educación, Cultura y Deporte, que regula la matriculación, evaluación y acreditación académica del alumnado de Formación Profesional en los centros docentes de la Comunidad Autónoma de Aragón.*
- *RESOLUCIÓN de 21 de noviembre de 2019, del Director General de Innovación y Formación Profesional, por la que se modifica la Resolución de 6 de marzo de 2018, del Director General de Planificación y Formación Profesional, por la que se dictan instrucciones para la ejecución y aplicación el desarrollo de la Orden de 26 de octubre de 2009, de la Consejera de Educación, Cultura y Deporte, que regula la matriculación, evaluación y acreditación académica del alumnado de Formación Profesional en los centros docentes de la Comunidad Autónoma de Aragón.*
- *ORDEN ECD/518/2022, de 22 de abril, por la que se regulan la evaluación y la promoción en la Educación Primaria, así como la evaluación, la promoción y la titulación en la Educación Secundaria Obligatoria, el Bachillerato y la Formación Profesional en los centros docentes de la Comunidad Autónoma de Aragón.*

En relación con la evaluación cabe destacar:

- La evaluación se realizará a lo largo de todo su proceso formativo y diferenciada para cada uno de los módulos profesionales que conforman el ciclo formativo.
- Los criterios de evaluación de los módulos profesionales que conforman cada uno de los ciclos formativos de las enseñanzas de formación profesional y los objetivos generales del ciclo serán los referentes fundamentales para valorar el grado de consecución de los resultados de aprendizaje de los mismos.



- Convocatorias: Este módulo, al impartirse en el segundo curso tiene dos convocatorias, la primera convocatoria será en marzo, antes de empezar el periodo de las FCT's y la segunda convocatoria tendrá lugar en junio.

En el régimen de enseñanza presencial, la evaluación continua del proceso formativo requiere la asistencia regular a las actividades lectivas programadas en los distintos módulos, el número de faltas de asistencia que determina la pérdida del derecho a la evaluación continua es como máximo del 15% respecto a la duración total del módulo profesional. De este porcentaje podrán quedar excluidos los alumnos que tengan que conciliar el aprendizaje con la actividad laboral, que deberán acreditar convenientemente. En este módulo son 16 faltas (horas).

6.2. Relación entre los resultados de aprendizaje y criterios de evaluación

A continuación, se establecen los criterios de evaluación de este módulo relacionados con los resultados de aprendizaje y las unidades didácticas. Se han **sombreado aquellos criterios de evaluación que se consideran mínimos** para alcanzar los resultados de aprendizaje y obtener evaluación positiva en el módulo:

Resultados de aprendizaje	Criterios de Evaluación	Unidades
1. Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades.	a) Se ha valorado la importancia de mantener la información segura.	Und.1
	b) Se han descrito las diferencias entre seguridad física y lógica.	Und.1
	c) Se han definido las características de la ubicación física y condiciones ambientales de los equipos y servidores	Und.3
	d) Se ha identificado la necesidad de proteger físicamente los sistemas informáticos.	Und.1,3
	e) Se ha verificado el funcionamiento de los sistemas de alimentación ininterrumpida.	Und.3
	f) Se han seleccionado los puntos de aplicación de los sistemas de alimentación ininterrumpida.	Und.3
	g) Se han esquematizado las características de una política de seguridad basada en listas de control de acceso.	Und.5
		Und.5



PROGRAMACIÓN DIDÁCTICA

Resultados de aprendizaje	Criterios de Evaluación	Unidades
	<p>h) Se ha valorado la importancia de establecer una política de contraseñas.</p> <p>i) Se han valorado las ventajas que supone la utilización de sistemas biométricos.</p>	Und.5
2. Gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando las técnicas para asegurar la integridad de la información.	<p>a) Se ha interpretado la documentación técnica relativa a la política de almacenamiento.</p> <p>b) Se han tenido en cuenta factores inherentes al almacenamiento de la información (rendimiento, disponibilidad, accesibilidad, entre otros).</p> <p>c) Se han clasificado y enumerado los principales métodos de almacenamiento incluidos los sistemas de almacenamiento en red.</p> <p>d) Se han descrito las tecnologías de almacenamiento redundante y distribuido.</p> <p>e) Se han seleccionado estrategias para la realización de copias de seguridad.</p> <p>f) Se ha tenido en cuenta la frecuencia y el esquema de rotación.</p> <p>g) Se han realizado copias de seguridad con distintas estrategias.</p> <p>h) Se han identificado las características de los medios de almacenamiento remotos y extraíbles.</p> <p>i) Se han utilizado medios de almacenamiento remotos y extraíbles.</p>	Und.4 Und.1,4 Und.4 Und.4 Und.4 Und.4 Und.4 Und.4 Und.4



PROGRAMACIÓN DIDÁCTICA

Resultados de aprendizaje	Criterios de Evaluación	Unidades
	<p>j) Se han creado y restaurado imágenes de respaldo de sistemas en funcionamiento.</p> <p>k) Se han aplicado medidas de seguridad de cifrado y encriptación a las copias de seguridad</p>	Und.2,4
3. Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.	<p>a) Se han seguido planes de contingencia para actuar ante fallos de seguridad.</p> <p>b) Se han clasificado los principales tipos de software malicioso.</p> <p>c) Se han realizado actualizaciones periódicas de los sistemas para corregir posibles vulnerabilidades.</p> <p>d) Se ha verificado el origen y la autenticidad de las aplicaciones que se instalan en los sistemas.</p> <p>e) Se han instalado, probado y actualizado aplicaciones específicas para la detección y eliminación de software malicioso.</p> <p>f) Se han aplicado técnicas de recuperación de datos.</p>	Und.1,5 Und.5,6,7 Und.5,6,7 Und.5,6,7 Und.5,6,7 Und.5,6,7
4. Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.	<p>a) Se ha identificado la necesidad de inventariar y controlar los servicios de red.</p> <p>b) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos y robos de información.</p> <p>c) Se ha deducido la importancia de minimizar el volumen de tráfico</p>	Und.6 Und.5 Und.5



PROGRAMACIÓN DIDÁCTICA

Resultados de aprendizaje	Criterios de Evaluación	Unidades
	generado por la publicidad y el correo no deseado.	
	d) Se han aplicado medidas para evitar la monitorización de redes cableadas.	Und.6,7
	e) Se han clasificado y valorado las propiedades de seguridad de los protocolos usados en redes inalámbricas.	Und.6
	f) Se han aplicado medidas para evitar la conexión no autorizada a redes inalámbricas	Und.6
	g) Se han descrito sistemas de identificación como la firma electrónica, certificado digital, entre otros.	Und.2
	h) Se ha instalado y configurado un cortafuegos en un equipo o servidor.	Und.7



Resultados de aprendizaje	Criterios de Evaluación	Unidades
5. Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento	<ul style="list-style-type: none">a) Se ha descrito la legislación sobre protección de datos de carácter personal.b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.d) Se ha contrastado la obligación de poner a disposición de las personas los datos personales que les conciernen.e) Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.f) Se han contrastado las normas sobre gestión de seguridad de la información.	U N I D A D 1

6.3. Instrumentos y procedimientos de evaluación

El proceso de evaluación se realiza de forma continua a lo largo de todo el curso. En dicho periodo se distinguen las siguientes fases:

1.- Inicial, en la que se recoge información sobre los conocimientos previos del alumno al principio de curso. Nos permite adaptar el comienzo de curso y conocer el grado de homogeneidad del grupo. La presencia de alumnos con necesidades de atención específica debe ser comunicada por los responsables del centro en esta fase y, en caso de tener alumnos con estas características, preparar las adaptaciones curriculares no significativas que proceda.

El módulo de Seguridad Informática es de segundo curso y por lo tanto todos los alumnos parten de un nivel mínimo, aunque se encuentran alumnos con materias pendientes de primero que pueden afectar el aprendizaje en el presente módulo.

Se reforzará el proceso de obtención de información para valorar los conocimientos de partida de los alumnos, a la vez que se explicarán conceptos básicos para minorar las deficiencias y homogeneizar el grupo.

2.- Sesiones de evaluación intermedias, que en éste módulo se realizará en el mes de diciembre. La calificación negativa del módulo conllevará a los alumnos

afectados la realización de actividades de refuerzo para superar aquellos contenidos y criterios de evaluación no superados y para afianzar el resto.

3.- Sesiones de evaluación final; los alumnos tienen dos convocatorias por curso, una en el mes de marzo y otra en el mes de junio. La superación del módulo conlleva la posibilidad de realizar la FCT, evidentemente condicionado por el resto de módulos del ciclo.

Los alumnos que suspendan la primera convocatoria dispondrán de un plan de actividades.

Por otro lado, para obtener información sobre el proceso de aprendizaje de los alumnos se podrán utilizar diversas técnicas o instrumentos de evaluación. Se seleccionarán aquellos instrumentos que se consideren más adecuados en cada momento. Entre los instrumentos de evaluación a utilizar cabe citar:

- Prueba inicial realizada a principio de curso para comprobar los conocimientos previos que tienen los alumnos/as.
- Pruebas escritas de carácter teórico práctico de las unidades de cada trimestre.
- Pruebas prácticas con ordenador (un ordenador por alumno) de las unidades didácticas correspondientes a cada trimestre.
- Prácticas individuales o en grupo propuestas en clase. Estas prácticas consistirán en la resolución de problemas, casos prácticos y simulación de casos reales. Estas prácticas podrán tener una doble función; por un lado, la correcta resolución del problema y por otro la elaboración de una guía o manual que incluya los pasos a ejecutar para resolver un caso práctico ilustrado con capturas de pantalla.

El uso de dichos instrumentos de evaluación podrá incorporar la realización de esquemas, tablas, mapas conceptuales o diagramas de flujo cuando proceda.

6.4. Criterios de calificación

Criterios aplicables a los alumnos que no hayan perdido el derecho a la evaluación continua.

Cada ejercicio o prueba realizada se evaluará de 0 a 10 puntos. Para obtener la **nota de cada trimestre** se utilizarán todos los ejercicios y pruebas puntuadas, realizando el siguiente desglose:

- | | |
|---------------------------------------|------|
| • Pruebas de valoración de contenidos | 80 % |
| • Prácticas individuales o en grupo | 20 % |

Para superar una evaluación es necesario haber obtenido una calificación media ponderada de los tres conceptos igual o superior a 5.

Los decimales en las notas se guardan para hacer las medias finales. Se truncan para la nota de la evaluación, por ejemplo, un 5.93, quedará como un 5.

La **notal final** del módulo se calculará de la haciendo la media aritmética de las dos evaluaciones trimestrales.

Será necesario obtener al menos una calificación de 4 en cada una de las pruebas para promediar. Todas las evaluaciones deberán haberse superado, es decir se habrá alcanzado una media de 5 en cada una de ellas.

Pruebas de valoración de contenidos

La nota de las pruebas de valoración se calculará de la siguiente manera:

- 60% Media aritmética de las pruebas escritas.
- 40% Media aritmética de las pruebas prácticas.

El alumno debe conseguir una nota de 4 puntos en cada prueba como mínimo para poder promediar.

En el caso de no haber realizado ninguna prueba práctica durante la evaluación la nota será el 100% del valor de las pruebas escritas.

La participación en la copia total o parcial en cualquier prueba de valoración de contenidos implicará una calificación de 0 en dicha prueba.

Prácticas individuales o en grupo

Las calificaciones de los distintos trabajos y actividades de cada evaluación serán promediadas para obtener la parte de la nota correspondiente a “Prácticas individuales o en grupo propuestas en clase”.

Las prácticas deberán entregarse en la fecha señalada. Se valorarán con una nota entre 0 y 10 atendiendo a la consecución de los objetivos planteados en la práctica, así mismo se valorarán las buenas prácticas de programación, la presentación, la limpieza, el orden y el grado de autonomía. Se dará feedback de la evaluación de la práctica al alumno y se permitirán entregas adicionales con mejoras sobre la entrega inicial siempre que estas entregas estén dentro de la fecha límite de entrega de cada práctica.

La participación en la copia total o parcial de cualquier trabajo implicará una calificación de 0 en el trabajo.

Las prácticas entregadas fuera de tiempo no podrán ser puntuadas en ningún caso con una nota superior a 5.

El máximo número de prácticas fuera de tiempo que podrá tener derecho el alumno a ser corregidas, por semana, serán dos.

6.5. Recuperación

La recuperación se establecerá para aquellas personas que no hayan obtenido los resultados de aprendizaje mínimos establecidos según los criterios de evaluación. Aquellos que no hayan alcanzado al menos un cuatro sobre diez en la calificación de las pruebas de contenidos conceptuales y procedimentales previstas, llevarán a cabo una recuperación de las mismas.

La recuperación consistirá en la realización de las pruebas teórica y práctica (que serán del mismo tipo que las especificadas en el apartado “6.3 Instrumentos y

procedimientos de Evaluación”). Los alumnos deberán realizar las pruebas que no hubieran superado y/o entregar las prácticas pendientes.

Se realizará una recuperación por cada evaluación tras la finalización de la segunda evaluación.

La no superación de este módulo antes de la realización de las FCT's, supone que el alumno/a no pueda realizarlas. Para estos alumnos se realizará una convocatoria en junio.

Los resultados de aprendizaje mínimos y los criterios de evaluación y calificación serán los establecidos en la presente programación.

Para aquellos alumnos que no hayan superado el módulo en la evaluación final celebrada en marzo, primera convocatoria, se les proporcionarán los medios y actividades para que puedan superar la segunda convocatoria que se realizará en la sesión de evaluación final de junio. En concreto se ha propuesto lo siguiente:

- Realización de ejercicios de apoyo, problemas, trabajos, casos prácticos y la resolución de las pruebas realizadas a lo largo del curso.
- Clases de apoyo durante el tercer trimestre

6.6. Evaluación de alumnos que hayan perdido el derecho a evaluación continua

Los alumnos que hayan perdido el derecho a la evaluación continua deberán realizar una prueba final representativa de todos los resultados de aprendizaje del módulo.

La nota final del módulo se calculará de la siguiente manera:

- 60% Prueba escrita.
- 40% Prueba práctica.

siendo necesario obtener al menos un 4 en cada una de las pruebas para promediar.

6.7. Evaluación final y evaluación extraordinaria

Evaluación final ordinaria

Los alumnos que no hayan perdido el derecho a la evaluación continua y que hayan superado durante el curso todas las unidades didácticas se les aplicará los criterios establecidos previamente en este apartado para el cálculo de la nota final del módulo.

Los alumnos que no hayan perdido el derecho a la evaluación continua pero no hayan superado todas las unidades didácticas podrán elegir entre dos opciones:

1ª) La realización de pruebas teórica y práctica independientes por cada evaluación suspendida. A partir de las notas obtenidas en cada una de estas pruebas y las notas de

las evaluaciones superadas durante el curso, se aplicarán los criterios establecidos previamente en este apartado para el cálculo de la nota final del módulo.

2ª) Realización de las mismas pruebas y aplicación de los mismos criterios que los alumnos que hayan perdido la evaluación continua.

Evaluación final extraordinaria

La evaluación extraordinaria constará de una única prueba representativa de todos los resultados de aprendizaje del módulo

La nota final del módulo se calculará de la siguiente manera:

- 60% Prueba escrita.
- 40% Prueba práctica.

siendo necesario obtener al menos un 4 en cada una de las pruebas para promediar.

El profesor orientará y apoyará a los alumnos que no superen el módulo en la evaluación final ordinaria y deban presentarse a la evaluación final extraordinaria. El apoyo consistirá básicamente en la realización de clases de repaso a lo largo del tercer trimestre y, en aquellos casos que lo necesiten, se proporcionará material adicional al entregado a lo largo del curso (documentación, ejercicios, prácticas, etc.).

6.8. Evaluación de la práctica docente y del proceso de enseñanza

Se hace necesaria una evaluación del propio proceso educativo, de la acción docente y de la programación, para ello se prevén los siguientes instrumentos:

a) Revisión del cumplimiento de los objetivos y la secuenciación al concluir cada unidad didáctica, para ello se hará uso del diario del profesor.

b) Se realizará un seguimiento periódico, al menos una vez al mes, del avance de la programación que permitirá detectar problemas y posibles desviaciones de forma que se puedan plantear acciones para responder a dichas desviaciones. Este seguimiento proporcionará información muy valiosa de cara a elaborar la memoria final del curso y la programación del curso siguiente.

c) Memoria de final de curso.

Todo el proceso de evaluación, en sus distintos aspectos, debe servir para reflexionar, cambiar lo inadecuado y mejorar año a año los métodos, objetivos y contenidos de la programación.

7. ACTIVIDADES DE ORIENTACIÓN Y APOYO ENCAMINADAS A LA SUPERACIÓN DE LOS MÓDULOS PROFESIONALES PENDIENTES

No aplica



8. EDUCACIÓN EN VALORES

Los temas de educación en valores aparecen incluidos en la programación en formas distintas según sea el tema de la forma siguiente:

EDUCACIÓN EN VALORES	ACTITUDES, VALORES, NORMAS Y HÁBITOS
Educación para la Salud	En el centro hay que crear unos hábitos de higiene física, mental y social que desarrollen la autoestima y mejoren la calidad de vida.
Educación para el Consumidor	Visión del software libre como alternativa a productos comerciales. Estudio de las demandas de consumo en cuanto a desarrollo de aplicaciones informáticas, proporcionando al alumno una formación referente a las tendencias actuales del mercado
Educación para la Convivencia	La clase es el lugar idóneo para aprender actitudes básicas de convivencia: solidaridad, tolerancia, respeto a la diversidad y capacidad de diálogo y de participación. Este tema transversal se fomentará sobre todo en las actividades a desarrollar en grupo y en los debates que sobre un tema se puedan producir. Consideración por los materiales del aula. Asistencia a clase y puntualidad...etc.
Educación no sexista	Se basa principalmente en la utilización del lenguaje hablado y escrito, puesto que en esta profesión no existe claramente una discriminación sexista salvo la habitual en la sociedad
Educación ambiental	Profesionalmente no existen grandes iniciativas a realizar, salvo costumbres de trabajo que suponen un menor impacto ambiental: apagar los equipos cuando no se usan, no generar residuos y arrojarlos a lugares adecuados, uso de documentación en formato digital como medida para no malgastar el papel y reutilizarlo o reciclarlo.

9. RECURSOS DIDÁCTICOS Y BIBLIOGRAFÍA

Materiales a emplear

Hardware

Rev.: 14 Fecha: 13/10/2021

Este documento debe ser utilizado en soporte informático.

Las copias impresas no están controladas y pueden quedar obsoletas; por tanto, antes de usarlas debe verificarse su vigencia



- Aula con 28 equipos informáticos para los alumnos y uno para el profesor.
- Proyector multimedia.
- Componentes de redes y herramientas.

Software

- Virtualización con VirtualBox
- Sistemas Operativos: Windows 10 y Windows Server y distribuciones de Ubuntu (20.04) u otros sistemas de Linux.
- Software adicional de seguridad informática
- Aplicaciones ofimáticas: Microsoft Office y LibreOffice
- Moodle y Google Workspace

Otros materiales

- Fotocopias, pizarra, proyector e Internet.
- Apuntes y ejercicios elaborados por el profesor
- Vídeos de Intypedia
- Revistas especializadas
- Pendrives u otro tipo de soporte informático

Bibliografía

Libro de texto: *Seguridad Informática Antonio Postigo Palacios Ed. Paraninfo, 2020*

Otros libros:

- *Seguridad Informática Ignacio Triviño Mosquera Ed. Síntesis, 2019*
- *Seguridad Informática Jose Fabián Roa Buendía Ed. McGraw-Hill, 2013*
- *Seguridad Informática Editex, Purificación Aguilera.*
- *UNIX and LINUX system administration handbook. Evi Nemeth et al. Pearson. 5th Ed 2017*
- *Linux. Guía de instalación y administración Vicente López Camacho Ed McGraw Hill 2003*
- *Linux. Guía para administradores de redes Vatus, Dawson y Purdy Anaya O'Reilly 2005*

10. ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES

Siempre que sea posible se propondrán visitas a algún centro de cálculo o empresa donde los alumnos puedan observar cómo se lleva a cabo los procesos de seguridad.

Las actividades se realizarán de acuerdo con lo convenido en el departamento.



11. MEDIDAS DE ATENCIÓN A LA DIVERSIDAD.

Las medidas de atención a la diversidad se concretan en las adaptaciones curriculares no significativas y de acceso que puedan precisar los alumnos.

Para atender a los alumnos ACNEAE se estudiará cada caso en particular en coordinación con los Departamentos de Orientación y FOL.

Medidas de refuerzo

El objetivo de las medidas de refuerzo es ayudar a los alumnos con dificultades para superar con éxito la materia. El profesor sugerirá material de refuerzo que el alumno tendrá que realizar en casa y que se podrán comentar dentro de las horas de permanencia en el centro del profesor. Estas actividades de refuerzo no formarán parte de los instrumentos de evaluación y calificación que se han establecido en el módulo.

Medidas de ampliación

Las medidas de ampliación tienen como objetivo atender a las demandas de aquellos alumnos que superan ampliamente los objetivos generales. Las medidas de ampliación serán básicamente dos:

- Investigación por parte del mundo de temas no tratados en el aula.
- Profundización en temas tratados.

Todas estas medidas estarán guiadas por el profesor.

Cuando un alumno precise adaptaciones de acceso, una vez comunicadas a los profesores, se realizará una reunión del Departamento para adoptar, de acuerdo con los recursos disponibles, las medidas de adaptación de acceso necesarias para los alumnos afectados.

En el presente curso no se han detectado, ni se ha comunicado la presencia de alumnos con necesidad de específica de apoyo educativo, ni se han comunicado adaptaciones de acceso.



12. PLAN DE CONTINGENCIA

Ante circunstancias excepcionales que afectasen el desarrollo normal de la actividad docente se llevarán a cabo las siguientes acciones:

- En el departamento se dispondrá de diversos materiales que permitan la continuidad de la actividad del alumnado. Los recursos se almacenarán en el ordenador del profesor del aula, o en un servidor al que tenga acceso el profesor encargado de atender la contingencia.
- Si hay posibilidad, el profesor podrá enviar a través del correo electrónico o dejar materiales en Internet para que los alumnos accedan a ellos y puedan realizar las actividades que se propongan.

13. PUBLICIDAD DE LA PROGRAMACIÓN

Al comienzo del curso, en la primera sesión con los alumnos, se les informa de los aspectos generales del módulo y de la normativa que establece el currículo del ciclo, haciendo un repaso de los objetivos, las competencias profesionales, los contenidos que se impartirán, etc.; y una vez aprobada por el Departamento se informará con detalle de la misma.

En dicha sesión se les comunica que, una vez aprobada la programación didáctica del módulo de Seguridad Informática correspondiente al presente curso, se dedicará una sesión de clase para dar a conocer, con especial dedicación, aquellos aspectos relacionados con el proceso de evaluación y se dará respuesta a las dudas que se puedan plantear.

La programación se publicará en la página Web del centro, en el tablón de anuncios del aula, o en el tablón de anuncios del Departamento de Informática y Comunicaciones.



14. MODIFICACIONES DE LA VERSIÓN 13

Se han realizado cambios en la numeración de los apartados para adecuarlos a la plantilla proporcionada por el Departamento de Calidad.

Se han realizado modificaciones a los apartados:

- 4.4 Distribución horaria UDs
- 6.1. Base legal
- 6.4. Criterios de calificación
- 6.5. Recuperación
- 6.7. Evaluación final y evaluación extraordinaria
- 9. RECURSOS DIDÁCTICOS Y BIBLIOGRAFÍA
- Eliminación del Anexo I referente al COVID